IN THE CLAIMS:

Please cancel claims 1-5 and 26-29 without prejudice to Applicant's right to seek allowance of said claims in a related application.

Please amend claims as indicated below.

Claims 1-5 canceled without prejudice

6. (currently amended) A method for protecting a digital signal, comprising the steps of:

providing a ~~the~~ digital signal ~~including~~ comprising digital data and ~~samples in a~~ file format information; ~~having an inherent granularity, comprising the step of:~~

creating a predetermined key that manipulates the file format information~~comprised of a transfer function-based mask set to manipulate data at the inherent granularity of the file format of the underlying digitized samples~~; and

manipulating the file format information using the predetermined key.

7. (original) The method of claim 6, wherein the digital signal represents a continuous analog waveform.

8. (original) The method of claim 6, wherein the predetermined key comprises a plurality of mask sets.

9. (original) The method of claim 6, wherein the digital signal is a message to be authenticated.

10. (currently amended) The method of claim 6, wherein the predetermined key comprises ~~mask set is ciphered by~~ a key pair comprising a public key and a private key.

11. (original) The method of claim 6, further comprising the step of:

using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

12. (original) The method of claim 6, wherein the digital signal represents a still image, audio or video.

13. (currently amended) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the steps of:

~~selecting the mask set, including one or more masks having random or pseudo-random series of bits; and~~

validating the one or more mask sets ~~at the start of the transfer function-based mask set~~before manipulating the file format information using the predetermined key.

14. (currently amended) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the steps of:

~~selecting the mask set, including one or more masks having random or pseudo-random series of bits; and~~

validating the one or more mask sets ~~at the start of the transfer function-based mask set~~before manipulating the file format information using the predetermined key.

15. (currently amended) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the steps of:

~~selecting the mask set, including one or more masks having random or pseudo-random series of bits; and~~

generating a hash value using the one or more masks sets; and

authenticating the one or more mask sets by comparing the generated ~~a~~ hash value with a predetermined ~~computed at the start of the transfer function-based mask set with a determined transfer function of the~~ hash value.

16. (currently amended) The method of claim 13, wherein said step of validating comprises the steps of:

generating a digital signature using the one or more mask sets; and

comparing the digital signature with a predetermined digital signature.

~~comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.~~

17. (currently amended) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the ~~steps~~ step of:

~~selecting the mask set, including one or more masks having random or pseudo-random series of bits; and~~

authenticating the one or more mask sets by comparing a generated digital signature ~~at the start of the transfer function-based mask set~~ with a predetermined ~~transfer function of the~~ digital signature.

18. (original) The method of claim 13, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal; and

wherein said step of validating is dependent on validation of the embedded information.

19. (currently amended) The method of claim 6, further comprising the step of:

computing a secure way hash function of carrier signal data in the digital signal, wherein the has function is insensitive to changes introduced into the carrier signal ~~for the purpose of carrying the transfer function-based mask set~~ during file format manipulation.

20. (currently amended) A method for protecting a digital signal, ~~the digital signal including digital samples in a file format having an inherent granularity,~~ comprising the steps of:

providing a digital signal comprising digital data and file format information;

creating a predetermined key ~~comprised~~ comprising a mask set ~~of a transfer function-based mask set that can manipulate data at the inherent granularity of the file format of the underlying digitized samples~~;

manipulating the file format information using the predetermined key;

authenticating the predetermined key ~~containing the correct transfer function-based mask set~~ during playback of the digital data; and

metering the playback of the digital data to monitor content.

21. (currently amended) The method of claim 20, wherein the predetermined key is authenticated to authenticate message information.

22. (currently amended) A method to prepare for the scrambling of a sample stream of data, comprising the steps of:

generating a plurality of mask sets to be used for encoding, including a random primary mask, a random convolution mask and a random start of message delimiter;

obtaining file format information about the sample stream of data; ~~a transfer function to be implemented;~~

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of the message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting a message size equal to the total number of bits in the message bit stream.

23. (original) A method to prepare for the encoding of stega-cipher information into a sample stream of data, comprising the steps of:

generating a mask set to be used for encoding, the set including a random primary mask, a random convolution mask, and a random start of message delimiter;

obtaining a message to be encoded;

compressing and encrypting the message if desired;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting the message size equal to the total number of bits in the message bit stream.

24. (original) The method of claim 23 wherein the sample stream of data has a plurality of windows, further comprising the steps of:

calculating over which windows in the sample stream the message will be encoded;

computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and

encoding the computed hash values in an encoded stream of data.

Claims 25-29 (canceled without prejudice)

30. (new) A method for protecting digital data, where the digital data signal is organized into a plurality of frames, each frame having i) a header comprising file format information and ii) at least a portion of the digital data, said method comprising the steps of:

creating a predetermined key to manipulate the file format information in one or more of the plurality of frames; and

manipulating the file format information using the predetermined key in at least two of the plurality of frames, such that the digital data will be perceived by a human as noticeably altered if it is played without using a decode key to restore the file format information to a prior state.

31. (new) The method of claim 30, wherein the predetermined key comprises a private key that is associated with a key pair.